WHAT IS CLAIMED IS:

1. A method of identifying unwanted messages, the method comprising:

inspecting a payload portion of a message being communicated and identifying characteristics of the payload portion;

comparing the characteristics of the inspected payload portion of the message with stored data indicating characteristics of at least one other message that has been inspected; and

identifying a security condition based on the comparison.

2. The method of claim 1 wherein the characteristics of the payload portion include information other than address information.

3. The method of claim 2 wherein the characteristics of the payload portion do not include address information.

4. The method of claim 1 wherein the message includes an electronic mail message.

5. The method of claim 1 further comprising rejecting the message if the security condition identified includes a hostile indicator.

6. The method of claim 5 wherein the security condition is identified as a hostile indicator when the comparison of the characteristics reveals a threshold number of messages having a shared characteristic.

7. The method of claim 6 further comprising removing previously-accepted messages having characteristics in common with subsequently-exchanged messages for which the security condition is identified as including the hostile indicator.

8. The method of claim 1 further comprising tracking the characteristics of the payload portion for comparison against characteristics of future messages, wherein the characteristics of a new message are compared with the characteristics of at least one message that has been tracked.

9. The method of claim 7 wherein comparing the characteristics of the payload portion includes comparing the characteristics of the payload portion of messages inspected with stored characteristics of other communicated messages.

10. The method of claim 7 wherein a message is tracked when the security condition is identified as including an indeterminate indicator.

11. The method of claim 10 wherein the indeterminate indicator is identified if the comparison of the characteristics does not itself reveal a hostile security condition, but the characteristics of the payload portion would reveal a hostile security condition in combination with similar characteristics of other messages.

12. The method of claim 10 further comprising accepting the message if the security condition includes the indeterminate indicator.

13. The method of claim 1 further comprising accepting the message if the security condition includes a neutral indicator.

14. The method of claim 1 wherein identifying the security condition includes comparing the characteristics of more than one message received by a single device.

15. The method of claim 1 wherein identifying the security condition includes comparing the characteristics of more than one message sent by a single device.

16. A method of identifying unwanted messages, the method comprising:

inspecting a message being communicated to a first device in a message exchanging system that includes two or more devices and identifying characteristics of the message;

comparing the characteristics of the message with stored data indicating characteristics of at least one other message communicated to a second device in the message exchanging system; and

identifying a security condition based on the comparison of the message inspected and the stored data.

17 The method of claim 16 wherein identifying the security condition includes comparing the characteristics of messages received by the more than one different device.

18. The method of claim 16 wherein identifying the security condition includes comparing the characteristics of messages sent by the more than one different device.

19. The method of claim 16 wherein the characteristics of the messages includes address information.

20. The method of claim 16 wherein the message includes an electronic mail message.

21. The method of claim 16 further comprising rejecting the message if the security condition is identified as including a hostile indicator.

22. The method of claim 21 wherein the security condition is identified as a hostile indicator when the comparison of the characteristics reveals a threshold number of messages having a shared characteristic.

23. The method of claim 22 further comprising removing previously-accepted messages if their characteristics share features with characteristics for subsequently exchanged messages for which the security condition is identified as including the hostile indicator.

24. The method of claim 16 further comprising tracking characteristics of the messages for comparison against characteristics of future messages, wherein the characteristics of a new message are compared with the characteristics of at least one message that has been tracked.

25. The method of claim 24 wherein comparing the characteristics of the messages inspected includes comparing the portion of the message inspected with a data store having characteristics of other communicated messages.

26. The method of claim 24 wherein a message is tracked when the security condition is identified as including an indeterminate indicator.

27. The method of claim 26 wherein the indeterminate indicator is identified if the comparison of the characteristics does not itself reveal a hostile security condition, but the

characteristics of the message would reveal a hostile security condition in combination with similar characteristics of other messages.

28. The method of claim 26 further comprising accepting messages when the indeterminate indicator is identified for the security condition.

29. The method of claim 16 further comprising accepting the message if the security condition includes a neutral indicator.